held 9/11-14/98 in Paris

OPEN PLATFORM INITIATIVE for MULTIMEDIA ACCESS (OPIMA)

Call for Proposals for Technologies

Please note that proposers should:

• Notify their intention to submit a proposal on or before close of business of 24 August 1998 to leonardo.chiariglione@cselt.it

• Send their contribution by email on or before close of business of 31 August 1998 to leonardo.chiariglione@cselt.it. The contribution must be in Word 6, HTML or PDF format.

Table of Contents

Intellectual Property Rights Statement

When submitting a proposal, authors must acknowledge that in case part or all of their proposal is included in OPIMA specifications and the included part contains patented items which are necessary for the implementation of OPIMA specifications, the IPR owners will accept the IEC/ISO/ITU practice for patented items in international standards. This amounts to either giving free use of the patented items, or giving licence on fair and reasonable terms and on a non-discriminatory basis.

Model for Intellectual Property Rights Statement

The following model holds the key language of the IEC/ISO/ITU Intellectual property rights statement. It may be used as a basis to provide the required IPR statement:

<Company Name> hereby declares that it is prepared to license its IPR, both granted and pending, which is necessary to manufacture, sell and operate implementations of OPIMA specifications.

<Company Name> also declares that it is willing to grant a licence to an unlimited number of applications throughout the world under reasonable terms and under conditions that are demonstrably free of any unfair competition.

<Signature>

<Name and function of responsible company representative>

Executive summary

This Call for Proposals is an invitation to submit proposals for platform technologies needed to realise the OPIMA goal of a system where the consumer is able to obtain a terminal and begin to consume and pay for multimedia services, without having prior knowledge of which services would be consumed, in a simple way such as by operating a remote control device.

These proposed technologies are intended to be utilised in the development of a specification that may be used by content and service providers, and by manufacturers to enable services satisfying the definition above. The time scale of specification development is 1999.

Those intending to submit a proposal(s) should consult Section 6 of this Call for Proposals.

1. Introduction

Recent developments in digital techniques have stimulated the deployment of digital services that are attractive to users by virtue of their ability to offer improved functionalities compared to those of analogue technologies.

Protection of content is of paramount importance for the success of these new services. The current environment is one in which content protection systems are designed and deployed on a proprietary basis. While this satisfies the concerns of individual service providers, it often discourages consumers because devices employed to decrypt signals can perform their function only for one or a reduced number of service providers. Therefore users can access different service providers only by acquiring multiple terminal devices.

The Open Platform Initiative for Multimedia Access (OPIMA) is based on the belief that the multimedia market would see a faster development if a standardised technology existed that would allow a user to consume and pay for services, without having prior knowledge of which services would be consumed, in a simple way such as by operating a remote control device. Fig. 1 below graphically depicts the goal of the OPIMA initiative in which the consumer is able to use a single terminal to access a multiplicity of services from multiple providers.

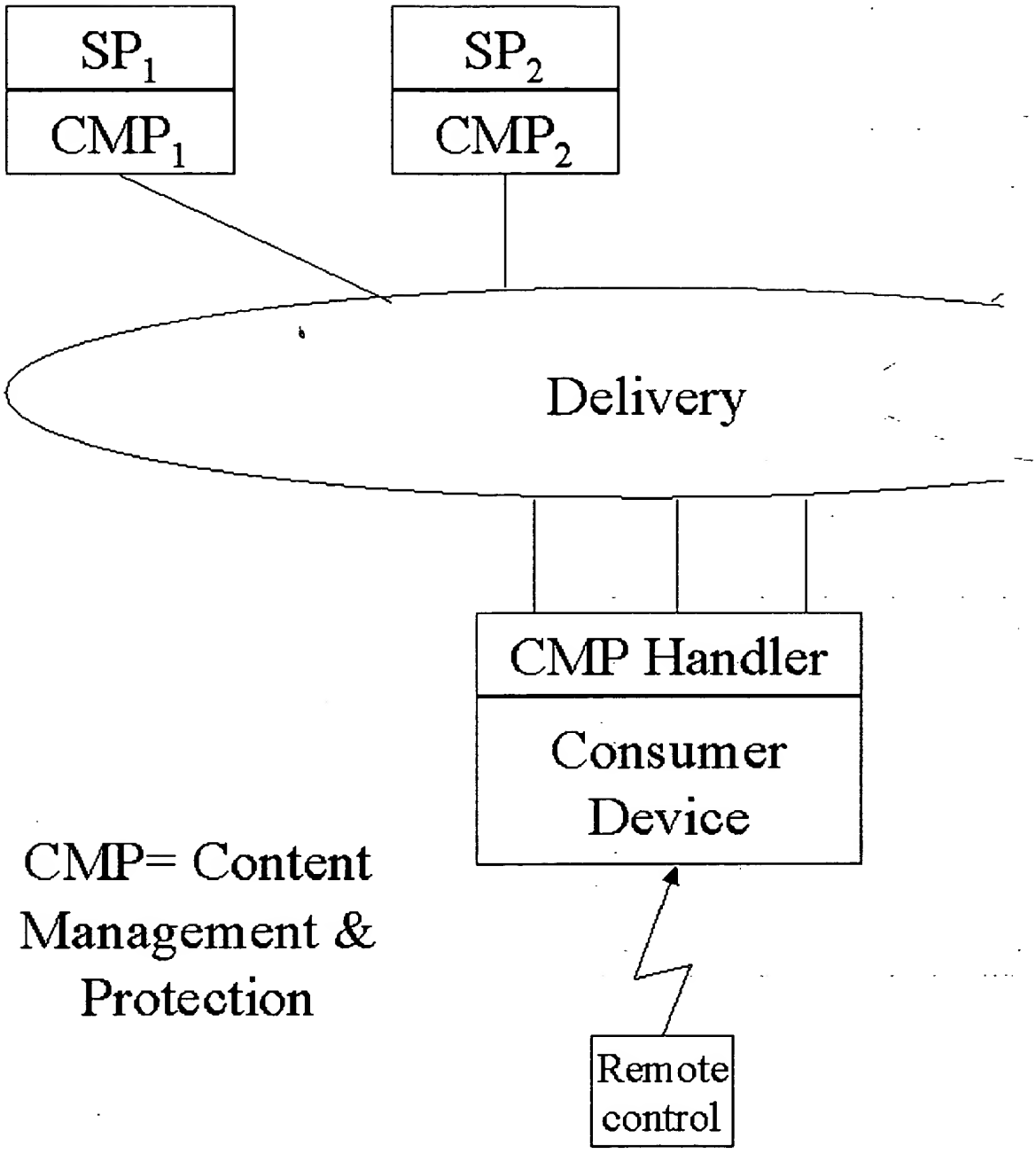


Fig. 1 - Graphical representation of the OPIMA goal

Even though the technology required to make possible the ideas described above exists, it is necessary to standardise some aspect of it in order to make the system work in an open manner. The international multi-industry OPIMA initiative has been established with the goal of achieving this standardisation. In this document "standardisation" is used to mean reaching industry agreement. It is envisaged that the OPIMA specification may be submitted to appropriate formal standards bodies for ratification.

This document has been developed by a group of industry representatives from different countries and

different components of the multimedia industry. It contains a list of possible applications and a list of requirements that it is believed need to be satisfied if the listed applications are to be supported. A very general reference model is given along with an analysis of how some of the existing solutions map onto the reference model.

The list of applications provided in this document is not necessarily exhaustive, and proposers may submit further applications if they feel that these would extend and improve the value of the specification. In this case proposers are invited to draw the attention to any additional requirements which arise from the additional applications.

The reference model has been kept at a very general level in order to minimise constraints placed upon any technology that a proposer may think appropriate. On the other hand proposers are invited to make the model more specific by providing further levels of detail of any technological components which would be appropriate for the attainment of the OPIMA goal.

This Call for Proposals is being widely disseminated to industry representatives and a wide range of responses is anticipated. At the September 1998 meeting the responses will be analysed and the technical work to develop the specifications will start. Current plans are that specifications will be frozen in September 1999.

While participants in the OPIMA initiative believe in the positive effect of the specifications on the development of the multimedia market, it is appreciated that different business models may require the use of proprietary systems. OPIMA has no intention of taking any action which would lead to the specifications becoming mandatory.

Participants in the OPIMA initiative are aware of the challenging nature of the current undertaking and invite all industry representatives sharing the OPIMA goal to join in this exciting technical development.

An electronic copy of this Call for Proposals can be found at

http://www.cselt.it/ufv/leonardo/opima

There is currently no plan to have a further call on the specific subject of this document. Therefore proposers should ensure that their contributions are submitted during this opportunity and comply with the deadlines specified.

2. OPIMA-enabled applications

2.1. List of Services to be supported

The services mentioned in this section serve as examples from which the requirements for the platform are derived. The specifications that OPIMA develops are targeted at supporting these services.

Note that while these examples imply certain business models, they do not make any assumption on the method of payment.

2.1.1. Required

Support for the following services and service models is required:

1. *Subscription TV/Audio*
2. *Pay-Per-Use*
3. *Near Video-on-Demand*
4. *Audio/Video-on-Demand*
5. *Services that add value* to those mentioned above – for example, paid-for Electronic Program Guides and other such services
6. *On-line multimedia services* – such as consuming services through the Internet
7. *Free TV/Radio* – the platform must allow free TV/Radio to be supported. *(Note that this is a requirement on the whole platform; not on any specific implementation. A service provider may choose an implementation that blocks the consumer device completely – and hence also block access to free TV/Radio – for example if a user does not pay for a subscription service)*

2.1.2. Optional

Additional services exist, which form an extension of the services mentioned under 'Required', and can be called 'Optional'. The following can be noted about these 'optionally supported services':

1. OPIMA believes the technology to allow the 'Required' services will naturally allow the 'Optional' services;
2. Technology proposed for supporting the Required services should not disallow the Optional services from being supported in the same system;
3. Proposals also supporting the Optional services, or allowing easy extension towards supporting them, will be evaluated more favourably than proposals only supporting the Required services.

These optionally supported services include:

- *Targeted advertising* – The user obtains permissions/credits in return for viewing advertising content
- *Rent-to-Own* – After paying *n* times, one can use the content for free (If $n = 1$, this becomes the 'Pay-One-Time-Fee' model)
- *Coupon Services* – The user gets a 'token' which may be used for using content, getting discounts, etc. The token can take many forms, for example a piece of software, a digital key, a smart card
- *Information services* – The content being obtained is not necessarily audiovisual. A few examples:
  - stock exchange information
  - traffic information
  - GPS information
- *Games* (single or multi user)
- *Software distribution* – It is believed that this is very similar to any other content distribution
- *Home shopping, home banking, gaming* – Services in which transactions play a role. Note that there is a clear connection between a television service (advertising) and home shopping
- *Auditing / Polling / Voting* – This means that a service provider can gain knowledge about the number of users accessing services and their degree of appreciation
- *Other services* – Please state which other services, not mentioned above, the proposal is also capable of supporting. Please address the question of how the proposal is open to newly developing services.

2.2. Benefit of the OPIMA approach to service integration

Currently a consumer who wants to access services from multiple providers is forced to have multiple terminals with different interfaces. This is an expensive and confusing situation, which slows down the adoption of digital services. The OPIMA initiative was launched to address this problem.

The OPIMA platform is primarily targeted to benefit consumers and service providers. Other players in the value network like rights holders, infrastructure and hardware providers may benefit from the platform as well, however always bearing in mind the benefits for the primary targets.

To encourage the provision of a greater selection of content to the consumer, the platform should guarantee the content providers' interests also through secure content management and protection and assurance of payment.

For a **consumer** it is of great benefit to have access to a platform that allows consumption of and easy payment for services, without having prior knowledge which services he would like to consume. For ease of use, these services should be provided on a single piece of equipment that is future-proof, following a consistent approach, controlled in a simple way such as by operating a remote control device. This consistent approach to services also relieves the consumer of complicated interaction concerning matters like authentication and payment.

For the **service provider** there is a standard interface to interact with all the terminals for all issues that deal with authentication, transaction processing and the like. Further, service providers could benefit from functionality like audits, polling, etc.

For the **hardware manufacturers** the OPIMA proposal offers the benefits of an open non-proprietary platform allowing fair competition. This of course also benefits the consumer.

It is recognised that the existence of such a platform would maximise the willingness of end users to consume content. This in turn would maximise content provisioning and globally enhance the role of **all legitimate actors** in the value network. The example of the GSM (Global System for Mobile) network and terminals has shown how standardisation can lead to economy of scale and enhanced service provision. It should be kept in mind, however, that the solution must be commercially viable and acceptable to the essential players in the network whose interests are impacted by any such solution.

It is important to note that OPIMA will propose specifications that interested parties are free to adopt. OPIMA does not intend to take any action which would lead to the specifications becoming mandatory.

3. Requirements

This section provides the requirements that guide the development of the OPIMA specifications. At the same time, it gives requirements for responses to this Call for Proposals (CfP). Sometimes a distinction is made between required support (usually denoted by the word 'shall') and optional support (usually expressed by using 'may').

3.1. Generic nature of the platform

The platform shall be as open as possible. In particular, the platform:

1. Preferably does not require proprietary hardware;
2. Preferably does not require a specific operating system.

3. Shall support multiple content management and protection systems (these individual content management and protection systems may, of course, use proprietary technologies, including hardware and software, as long as the interfaces conform to the OPIMA specifications).

3.2. Security and Privacy

The proposed platform needs to be secure and trustworthy. This means that:

1. The platform shall support identification and authentication of users and transactions (for example by digital contracts);
2. The platform shall prevent unauthorised access to information (i.e., access by parties that are not entitled to this information) and shall be robust against piracy. (Aspects of these requirements may be: preventing unauthorised copying of and access to content);
3. The platform shall support a means of assuring that users are only charged for services they have agreed to consume, and support giving the user an overview of the services consumed;
4. The platform shall support 'non-repudiation', i.e.:
   - provide proof that the user has agreed to order / consume the service;
   - provide proof of payment;
5. The platform shall support provision of accurate accounting information;
6. The platform may support – perhaps by providing some of the functionality listed above – binding negotiations. (This requirement refers to a model in which, if a party bids for goods or services using the platform, and the bid is accepted by the other party, this bid is equivalent to a purchase agreement.)

If different levels of security and robustness against piracy are allowed, systems with lower security levels shall never be able to compromise systems with higher security levels.

The platform shall support access control by

1. parental control;
2. jurisdictional and cultural policy (i.e., legal restrictions, possibly geographically determined).

The platform shall support service models in which the user's identity is not disclosed to the service provider and/or to other parties.

3.3. Connection type / form of interaction

This section lists requirements in the area of the type of connection and the form of interaction. Like before, there are requirements that *must* be supported, and extensions that, while they do not address the immediate focus of this Call for Proposals, do increase the value of the proposal.

The following types of connection shall be supported:

1. 1. Off-line consumption of content
2. 2. On-line consumption of content, for which are distinguished:

   a. Broadcast, with the following return channel characterisations:

   - i) without return channel

- ii) with intermittent return channel
- iii) with persistent return channel

b. Interactive, with the following return channel characterisations:

- i) symmetric and asymmetric bandwidth
- ii) similar or different paths to and from the user

It is understood that these models and their sub-categories are not mutually exclusive.

Along a slightly different axis describing the connection, the platform shall be able to support:

1. *One-to-one operation*; such as sending content from a service provider to a user;
2. *One-to-many operation*; such as sending content to multiple users on a broadcast network;
3. *Many-to-one operation*; such as when a user receives content from several service providers simultaneously; the collection of information constitutes one consistent service.

Along the same axis, proposals *may* also support:

1. *Many-to-many*, like in multi-party games, in which value is at stake.

The platform shall at least support:

1. service provider to customer operation.

In addition, it may also support:

1. customer-to-customer operation, in which value is transferred from one (end) user to another;
2. service provider to service provider operation.

3.4. Types of transactions

The platform shall allow a wide range of transaction models. At least the following types of transactions shall be supported:

1. prepaid;
2. postpaid;
3. subscription;
4. pay-per-use;
5. rent-to-own;
6. booking;
7. credit and debit;
8. end user pays; third party pays; service provider pays (possibly to the end user);
9. incremental purchase of permissions with respect to the same content, for example: one first obtains the permission to *view*, and afterwards the permission to *modify* or *copy*.

Both on-line and off-line connection modes are foreseen with these types of transactions. Please indicate which types of transactions are supported for each of the connection modes.

Note: again it is recognised that these transaction models are not mutually exclusive.

3.5. Device types

A device is a system that is used to access and consume information. In principle, the platform shall support any device that can be used to consume multimedia services. At least the following devices need to be supported:

1. Digital TV
2. Set top boxes
3. Local storage devices (e.g., DVD-RAM)
4. Digital Radio
5. Personal Computers
6. Mobile devices used to access multimedia services
7. Screen telephones.

Support for other (future) multimedia devices may also be considered.

3.6. Mobility

The platform shall support mobility. In particular, it shall:

1. support service models that allow terminal mobility, meaning that the user can use the same device in different locations;
2. have provisions for supporting user mobility across terminals, meaning that the users can move to a different terminal and keep their permissions to use the service.

While user mobility could be provided through 'personalisation' and the usage of 'user profiles', this issue is considered to be outside the scope of this Call.

3.7. List of Parties / Roles in the Value Network

The focus of OPIMA is currently on the relationship between

- the end user, and
- the service provider.

OPIMA recognises that many other roles exist in the value network. The platform shall not exclude the interests of these parties from being served.

While this Call for Proposals is not focused on these other parties, proposers are asked to state how their proposal affects the position of these other parties. Also, OPIMA asks proposers to assess how silent OPIMA and the proposed solution can be about the existence of these parties.

These parties include:

1. Hardware manufacturers
2. Security providers

3. Service brokers
4. Rights holders
   - on content
   - on algorithms (e.g., coding algorithms)
5. Infrastructure providers
6. Transaction infrastructure providers
7. Legitimate third parties (Third parties such as trusted third parties, tax authorities, regulatory agencies, *not* including parties like pirates)
8. The end user in the role of service provider.

It is understood that several of these roles can be unified in one entity.

4. Reference Architecture

4.1. The OPIMA approach to specifications

The figure below is a representation of the system addressed by OPIMA specifications. It comprises four entities: the Service Provider System (SP), the Service Provider Support (SP') as seen from the end-terminal perspective, the trusted middleware (TMW); and the Smart Card (SC). In principle, OPIMA specifications can address any subsystem in a similar context.

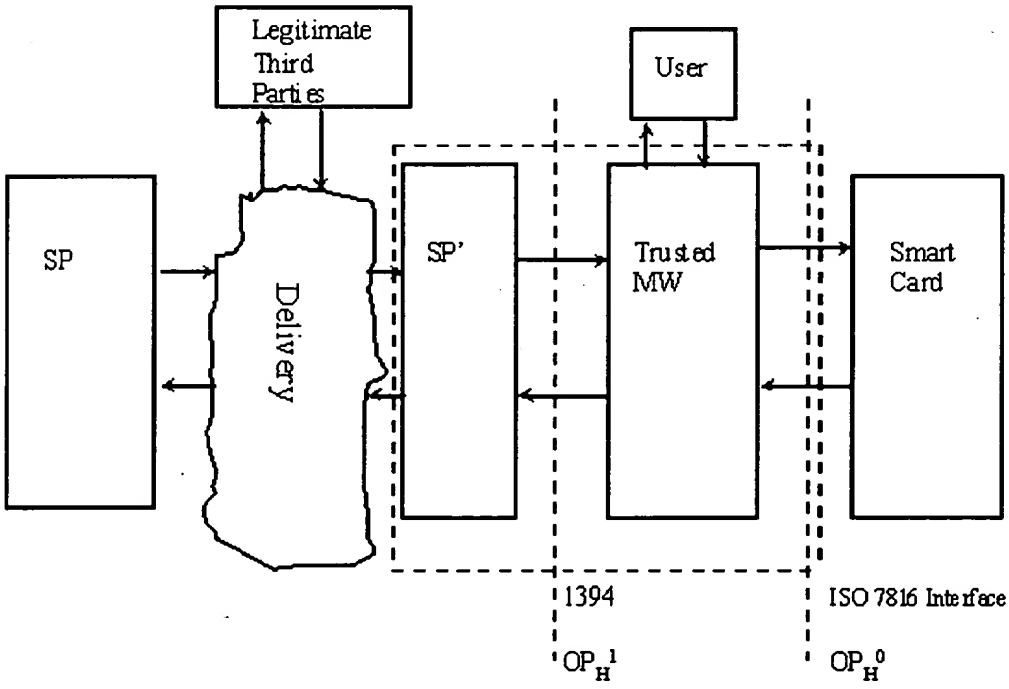


Fig. 2 - OPIMA Reference Model

Notes to the picture:

- *The 'H' in OP_HX refers to OPIMA Hardware*
- *Truted Middleware and Smart Card functions could also be carried together (e.g., on a PC card)*
- *Permissions are to be fully portable (e.g., on a Smart Card)*
- *Trusted Middleware is self-replaceable*
- *SP' is a generic service provider interface manufactured into every OPIMA device.*

Relocation of tools. Because OPIMA specifications have to satisfy business and service models of multiple industries, OPIMA tools need not only to be usable in a variety of different systems but also in different parts of the same systems. OPIMA defines its tools in such a way that they can be relocated, whenever this relocation is technically possible and practically meaningful.

OPIMA specifies the minimum. If the OPIMA reference model is mapped onto a particular application, the boundaries shown in the diagram may not be identifiable. As OPIMA addresses a multi-industry environment, it can only produce specifications of tools with the minimum of detail needed for interoperability.

The OPIMA architecture is intended to have longevity. The technologies used by OPIMA systems are targets for attack by illegal operators and interests. Therefore, the technology and the nature of the tools that will be used by OPIMA conformant systems require flexibility and the ability to replace components as they are compromised or when better technology becomes available.

4.2. Assumptions

The following assumptions reflect a basic rationale behind the elements of the OPIMA reference architecture:

Assumptions	Benefits
1. A secure and trusted environment in which all implementations are based	Service provider confidence
2. Intellectual property is protected	Content owner confidence
3. No predefined location and implementation of API's and hardware interfaces	Multiple instantiations of the architecture with a variety of exposed interfaces
4. Existence of user identification module	Unique identification of users whilst protecting privacy
5. Existence of a secure dynamic (distributed) registry for hardware and software interfaces	Uniform manufacturing; Local configuration and personalisation

4.3. Elements of the reference model

Smart Card (SC)

The smart card is viewed as the user identification and service enabling module. The smart card may be provided to a consumer by a Service Provider or an independent vendor. It should not be limited to enabling access to a single service provider or to a single application. The smart card should be a secure

environment in which the consumer is confident of its integrity. The currently known interface for smart card technology is given in ISO 7816 and its subchapters.

Service Provider System (SP) and Service Provider Support (SP')

The service provider is an entity which presents a unified image to a consumer who wishes to consume the services or products offered by the service provider. A service provider may have unique and proprietary applications requirements and interfaces. These are made transparent to the consumer by a secure download technology enabled by an OPIMA compliant terminal. This is accomplished by the presence of a generic (and secure) service provider support function (SP') in combination with a trusted middleware component (TMW) that is resident in each OPIMA compliant terminal at the time of manufacture.

Legitimate Third Party

A legitimate third party (LTP) is an entity whose presence in the system is authorised. This excludes unauthorised third parties such as pirates. The presence of an LTP is optional.

Trusted Middleware (TMW)

Trusted Middleware (TMW) is the core element in the system's ability to provide secure and trusted services. Only a certified middleware component has the ability to incorporate and certify additional or replacement functionalities including replacing itself in a trusted manner.

The trusted middleware component is capable of communicating with the smart card and the service provider support functions. The trusted middleware component manufactured within each OPIMA terminal contains the necessary functions to facilitate the addition of the Service Provider elements of the TMW. This can be achieved via secure download or other trusted methodology. The basic TMW, without any additional elements, will allow the operation of the basic functions for which the terminal is intended. For example, a digital television without these additional elements can receive and display free TV services.

Functions that are specific to individual Service Providers may be added to the basic TMW. This allows one or more service providers to offer available services on an OPIMA terminal. Security and application protection and management are required when additional service enabling is provided.

The SP' and TMW functionality may be combined in a single entity. If they are not, an interface such as IEEE 1394 may be used.

4.4. Known hardware Specifications

For the interfaces depicted in the diagram above, the following interfaces are known:

OP_H1	IEEE 1394 (CPT WG-1)
OP_H0	ISO 7816

5. Example implementations

In this section we show how two different implementations can be mapped onto the reference model above.

5.1. Global System for Mobile (GSM)

This section describes the application of a GSM-like Challenge/Response Scenario to the OPIMA Reference Model.

5.1.1. Description of GSM security mechanisms

The security services provided by GSM are:

- *Anonymity* – Making it difficult to identify the user of the system to parties that are not entitled to this information.
- *Authentication* – To identify the user to the service provider for billing purposes.
- *Signalling Protection* – To protect sensitive information on the transmission channel.
- *User Data Protection* – To protect the passing of user data across the network.

The use of a SIM (Subscriber Identity Module) card is central to the security model of GSM. The GSM system goes through a number of steps to ensure secure use of services:

- Equipment Authentication
- SIM Verification
- SIM Authentication
- Secure Payload Exchange.

1. Equipment Authentication

As each GSM Mobile Terminal has a unique identity (IMEI, International Mobile Equipment Identifier); the first step after connection to the service network is to check the terminal is not blacklisted.

2. SIM Verification

The purpose of this step is to increase probability that the SIM is in the hands of the correct user. This is done by prompting the user for a secret code (PIN), which is checked locally on the SIM.

3. SIM Authentication

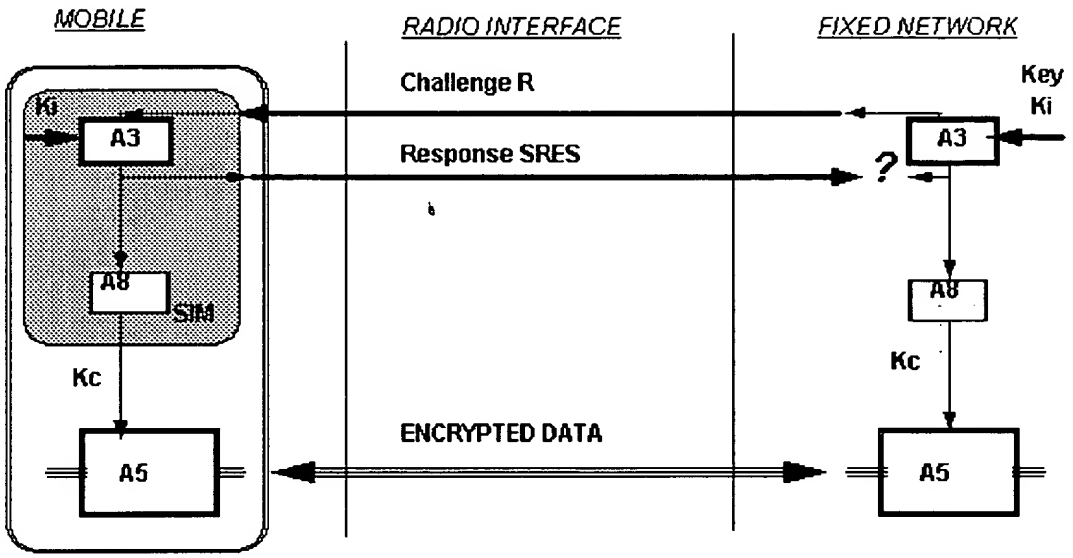
Authentication involves two functional entities: The SIM card in the Mobile Terminal and the Authentication database of the service provider. Each subscriber is given a secret key, a copy of which is stored in the SIM card and in the Authentication database. During the authentication process, the service provider generates a random number to the terminal. Both the mobile terminal and the service provider then use the random number and the secret key to compute, through a commonly agreed ciphering algorithm a so called Signed Response (SRES), which the mobile terminal sends back to the service provider. If the two computed numbers are the same, the subscriber is authenticated.

For authentication of Internet access over dial-up links where the PPP is used, a similar mechanism is used as defined in RFC 1994.

4. Secure Payload Exchange

The same SRES is then used to compute, using a second algorithm, a ciphering key that will be used for payload encryption / decryption, using a third algorithm.

The process is illustrated by the following diagram:



5.1.2. Mapping GSM system elements to OPIMA system elements

GSM	OPIMA
SIM	Smart Card / User Identification Module
Mobile Terminal (MT)	Consumer Device
MT Implementation	Trusted Middleware (TMW)
Currently no downloading - SIM Toolkit (future)	SP' (download)

GSM's Subscriber Identity Module corresponds to OPIMA's Smart Card, or, more generally, a OPIMA User Identification Module.

The OPIMA consumer device, including the software in it, corresponds to the GSM mobile terminal. The essential difference is that GSM terminals currently do not support software download from the service provider (although this is an ongoing development), which is on the other hand a crucial capability of the OPIMA consumer device.

For that reason, the TMW (Trusted Middleware) is mapped to the Mobile Terminal implementation, whereas the SP' element currently has no direct correspondence on the GSM model.

5.1.3. GSM-like authentication applied to OPIMA reference model

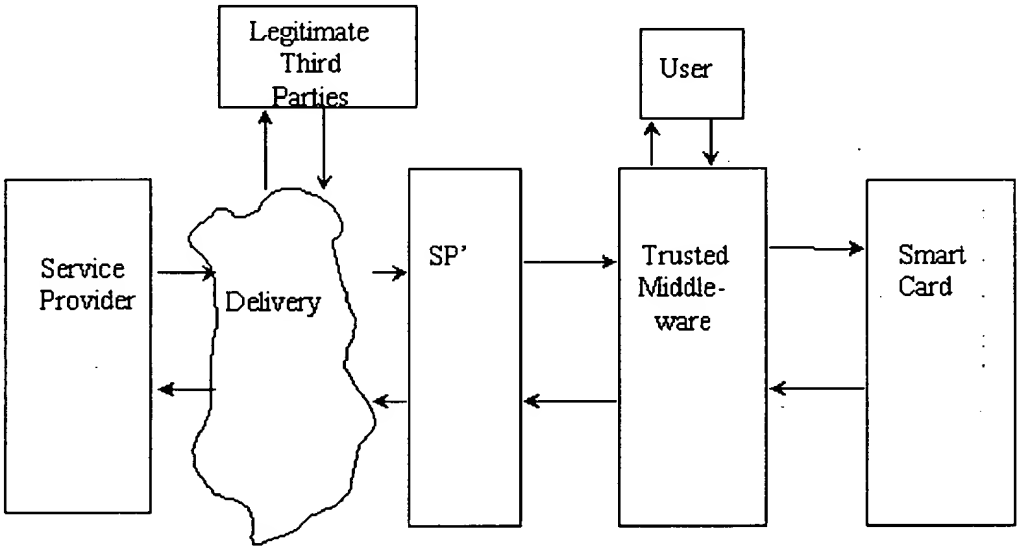
The user authentication procedure allowed by the OPIMA reference model is as follows:

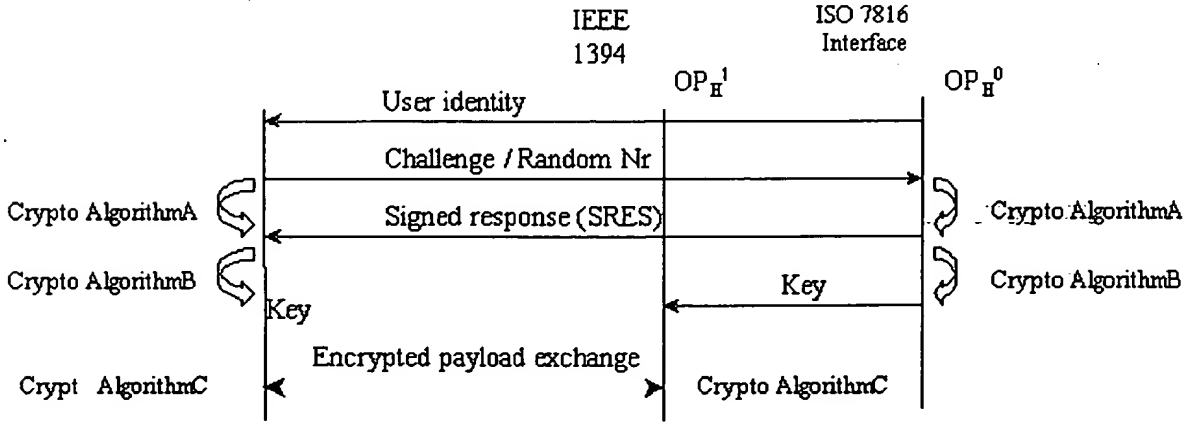
1. If the OPIMA consumer device is newly purchased without preloaded Service Provider specific elements, we assume the consumer device only has the basic capability to connect to some service

provider and to support basic secure download.

2. It is assumed that the Smart Card / User Identification Module is inserted in the consumer device.
3. The user is optionally asked for card verification, by prompting for entry of a secret code (PIN).
4. The consumer device connects to a service provider. It is assumed that the Smart Card was issued by the service provider and thereby determines the primary service provider the consumer device connects to.
5. The consumer device transmits the identity of the user (and optionally of the equipment) to the service provider.
6. The Service Provider transmits a random number to the consumer device in order to initiate user authentication.
7. The Trusted Middleware and the service provider simultaneously compute a Signed Response (SRES) from the random number and the user-specific secret key, using a commonly agreed algorithm.
8. The terminal sends the SRES to the service provider, who compares the two numbers.
9. If the two numbers are equal, the authentication was successful.
10. The same initial random number and subscriber key can be used to compute another key using another algorithm, to encrypt / decrypt payload if desired.

In the following interaction diagram, system elements which only pass information through such as the delivery network and the SP' component, are omitted.

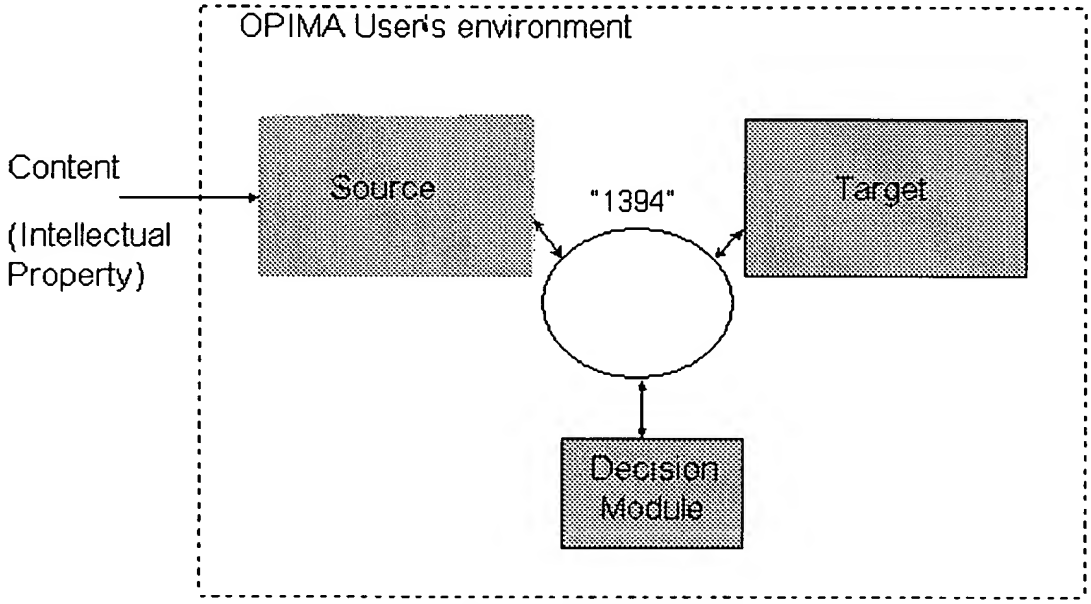




5.2. Intellectual Property Management and Protection Framework / "You Play-You Pay"

Another possible scenario for use of the OPIMA Reference Model is in providing protection and management of intellectual property, both in content and, potentially algorithms and other components of the environment.

Such uses highlight the potential diversity of the applications, as some intellectual property owners may wish to use only the most rudimentary protection schemes, whilst others may wish to employ much more complex approaches involving both management and protection.



Intellectual Property Manangement and Protection Framework

OPIMA User Environment: This could represent, for example, the user's home appliances, interconnected by a 1394-like bus, as being considered by the Multimedia Home Platform activity of the DVB project.

"1394" bus: Allows establishing of secure point-to-point channels (by performing authenticated key exchange (AKE) and encryption/decryption). [IEEE 1394]

Source: Is a device which receives content from outside the environment (e.g. by broadcast, internet, phone or physical media such as DVD disc). It could be, for example, a receiver or an Integrated Receiver/Decrypter (IRD).

Target: Is a device which is the final destination of the content where the content is consumed. It could be a digital television display or a recording device, such as DVD-RAM.

Decision Module: Is a device responsible for deciding whether the transmission of the content from the source to the target is permitted. In particular the decision module might verify the credentials of the other modules and the proper matching of authorizations to these credentials. These authorizations may come with the content over any of the available channels and must somehow be securely associated with the content. One possible implementation of the decision module is a tamper-resistant smart card which

allows periodic upgrades.

Any of the components above could be a software module in a PC.

How does intellectual property management and protection (IPMP) operate in this scenario? In the extreme case (referred to by some as "You Play, You Pay"), used mainly for illustration, the content may come entirely unencrypted, but the decision module may refuse transmission from source to target unless it receives also proper authorisations for this transmission (e.g. a receipt of purchase, which could have been received offline from a retail store or over the phone or stored on a user's personal smart credit card).

5.2.1. Possible extensions

The above scenario can, in principle, be generalized to an arbitrarily complex, dynamic, distributed architecture.

In this architecture the necessary components could be specified by authorizations and/or other modules received from any source, thereby supporting dynamically re-configurable webs of trust. In particular some of the components could be implemented and delivered as software which is then run on trusted virtual machines. In this way the overall system security and flexibility can be increased, forcing the prospective pirate to compromise multiple and possibly dynamic points of the system. The architecture could even support secure intelligent agents e.g. performing negotiations etc. This approach also allows decisions about the optimal configurations of the system to be decided dynamically by market forces.

5.2.2. Mapping the IPMP Framework to the OPIMA Reference Model

The Source receives Content (Intellectual Property) from the Delivery cloud in the OPIMA Reference Model (RM). The relevant parts of Source and Target (in this case the IEEE 1394 interface) are part of the Trusted MW which must be integrated into components outside of the OPIMA RM (e.g. a digital TV display). Both Source and Target could be either the SP' or part of the Trusted MW or a combination of these two. The Decision Module maps to the Smart Card component. In this example the Trusted MW component of the RM is distributed in a number of interconnected Consumer Electronics components.

6. Submission, Evaluation and Subsequent Specification Development

Parties interested in proposing technology to OPIMA should:

1. Notify their intention to submit a proposal on or before close of business of 24 August 1998 to leonardo.chiariglione@cselt.it.
2. Send their contribution by email on or before close of business of 31 August 1998 to leonardo.chiariglione@cselt.it. The contribution must be in Word 6, HTML or PDF format.

Submissions will be posted on a password protected Web page for access by OPIMA participants. Those who do not wish to have their submission posted should state so in their submission but still need to send an electronic copy to the address above. In this case proposers shall bring 100 paper copies to the meeting place.

INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC1/SC29/WG11
CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC1/SC29/WG11 N
MPEG 00/
October 2000

Source: **Leonardo Chiariglione - Convenor**
Title: **Short MPEG-2 description**

MPEG-2

Generic coding of moving pictures and associated audio information

MPEG-2 is a standard currently in 9 parts. The first three parts of of MPEG-2 have reached International Standard status, other parts are at different levels of completion. One has been withdrawn

- ISO/IEC 13818-1:2000 Information technology -- Generic coding of moving pictures and associated audio information: Systems (available in English only)
- ISO/IEC 13818-2:2000 Information technology -- Generic coding of moving pictures and associated audio information: Video (available in English only)
- ISO/IEC 13818-3:1998 Information technology -- Generic coding of moving pictures and associated audio information -- Part 3: Audio (available in English only)
- ISO/IEC 13818-4:1998 Information technology -- Generic coding of moving pictures and associated audio information -- Part 4: Conformance testing (available in English only)
- ISO/IEC 13818-4:1998/Cor 2:1998 (available in English only)
- ISO/IEC 13818-4:1998/Amd 1:1999 Advanced Audio Coding (AAC) conformance testing (available in English only)
- ISO/IEC 13818-4:1998/Amd 2:2000 System target decoder model (available in English only)
- ISO/IEC 13818-4:1998/Amd 3:2000 Additional audio conformance bitstreams (available in English only)
- ISO/IEC TR 13818-5:1997 Information technology -- Generic coding of moving pictures and associated audio information -- Part 5: Software simulation (available in English only)
- ISO/IEC TR 13818-5:1997/Amd 1:1999 Advanced Audio Coding (AAC) (available in English only)
- ISO/IEC 13818-6:1998 Information technology -- Generic coding of moving pictures and associated audio information -- Part 6: Extensions for DSM-CC (available in English only)

- ISO/IEC 13818-6:1998/Cor 1:1999 (available in English only)
- ISO/IEC 13818-6:1998/Amd 1:2000 Additions to support data broadcasting (available in English only)
- ISO/IEC 13818-6:1998/Amd 2:2000 Additions to support synchronized download services, opportunistic data services and resource announcement in broadcast and interactive services (available in English only)
- ISO/IEC 13818-7:1997 Information technology -- Generic coding of moving pictures and associated audio information -- Part 7: Advanced Audio Coding (AAC) (available in English only)
- ISO/IEC 13818-7:1997/Cor 1:1998 (available in English only)
- ISO/IEC 13818-9:1996 Information technology -- Generic coding of moving pictures and associated audio information -- Part 9: Extension for real time interface for systems decoders (available in English only)
- ISO/IEC 13818-10:1999 Information technology -- Generic coding of moving pictures and associated audio information -- Part 10: Conformance extensions for Digital Storage Media Command and Control (DSM-CC) (available in English only)

Part 1 of MPEG-2 addresses the combining of one or more elementary streams of video and audio, as well as, other data into single or multiple streams which are suitable for storage or transmission. This is specified in two forms: the Program Stream and the Transport Stream. Each is optimised for a different set of applications. A model is given in Figure 1 below.

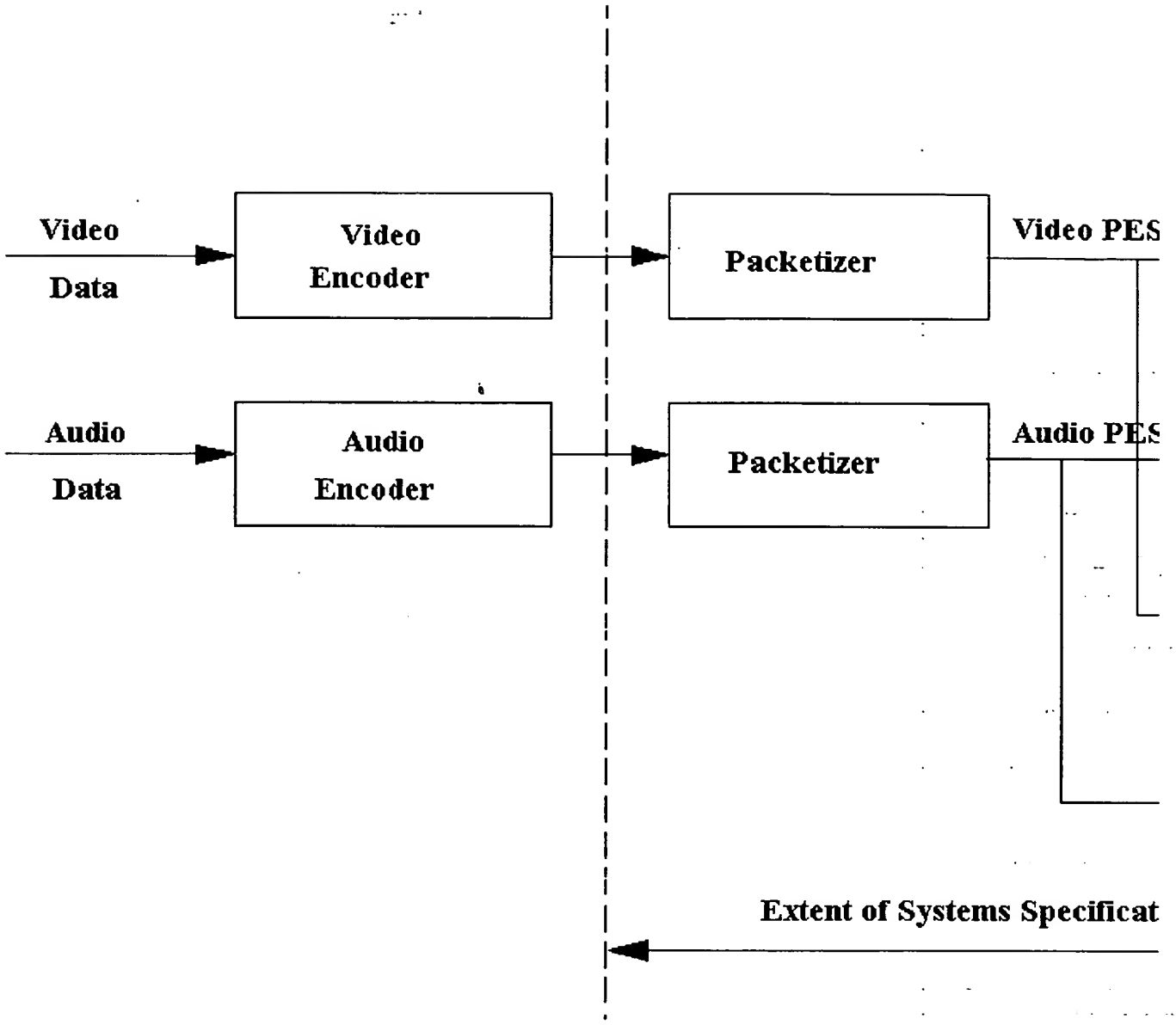


Figure 1 -- Model for MPEG-2 Systems

The Program Stream is similar to MPEG-1 Systems Multiplex. It results from combining one or more Packetised Elementary Streams (PES), which have a common time base, into a single stream. The Program Stream is designed for use in relatively error-free environments and is suitable for applications which may involve software processing. Program stream packets may be of variable and relatively great length.

The Transport Stream combines one or more Packetized Elementary Streams (PES) with one or more independent time bases into a single stream. Elementary streams sharing a common timebase form a program. The Transport Stream is designed for use in environments where errors are likely, such as storage or transmission in lossy or noisy media. Transport stream packets are 188 bytes long.

Part 2 of MPEG-2 builds on the powerful video compression capabilities of the MPEG-1 standard to offer a wide range of coding tools. These have been grouped in profiles to offer different functionalities. Only the combinations marked with an "X" are recognised by the standard.

Tab. 1 - MPEG-2 Video profiles

	Simple	Main	SNR scalable	Spatial scalable	High	Multiview	4:2:2
High level		X			X		
High-1440 level		X		X	X		
Main level	X	X	X		X	X	X
Low level		X	X				

Since the final approval of MPEG-2 Video in November 1994, one additional profile has been developed. This uses existing coding tools of MPEG-2 Video but is capable to deal with pictures having a colour resolution of 4:2:2 and a higher bitrate. Even though MPEG-2 Video was not developed having in mind studio applications, a set of comparison tests carried out by MPEG confirmed that MPEG-2 Video was at least good, and in many cases even better than standards or specifications developed for high bitrate or studio applications.

The 4:2:2 profile has been finally approved in January 1996 and is now an integral part of MPEG-2 Video.

The Multiview Profile (MVP) is an additional profile currently being developed. By using existing MPEG-2 Video coding tools it is possible to encode in an efficient way tow video sequences issued from two cameras shooting the same scene with a small angle between them. This profile will be finally approved in July 1996.

Part 3 of MPEG-2 is a backwards-compatible multichannel extension of the MPEG-1 Audio standard. Fig. 2 below gives the structure of an MPEG-2 Audio block of data showing this property.

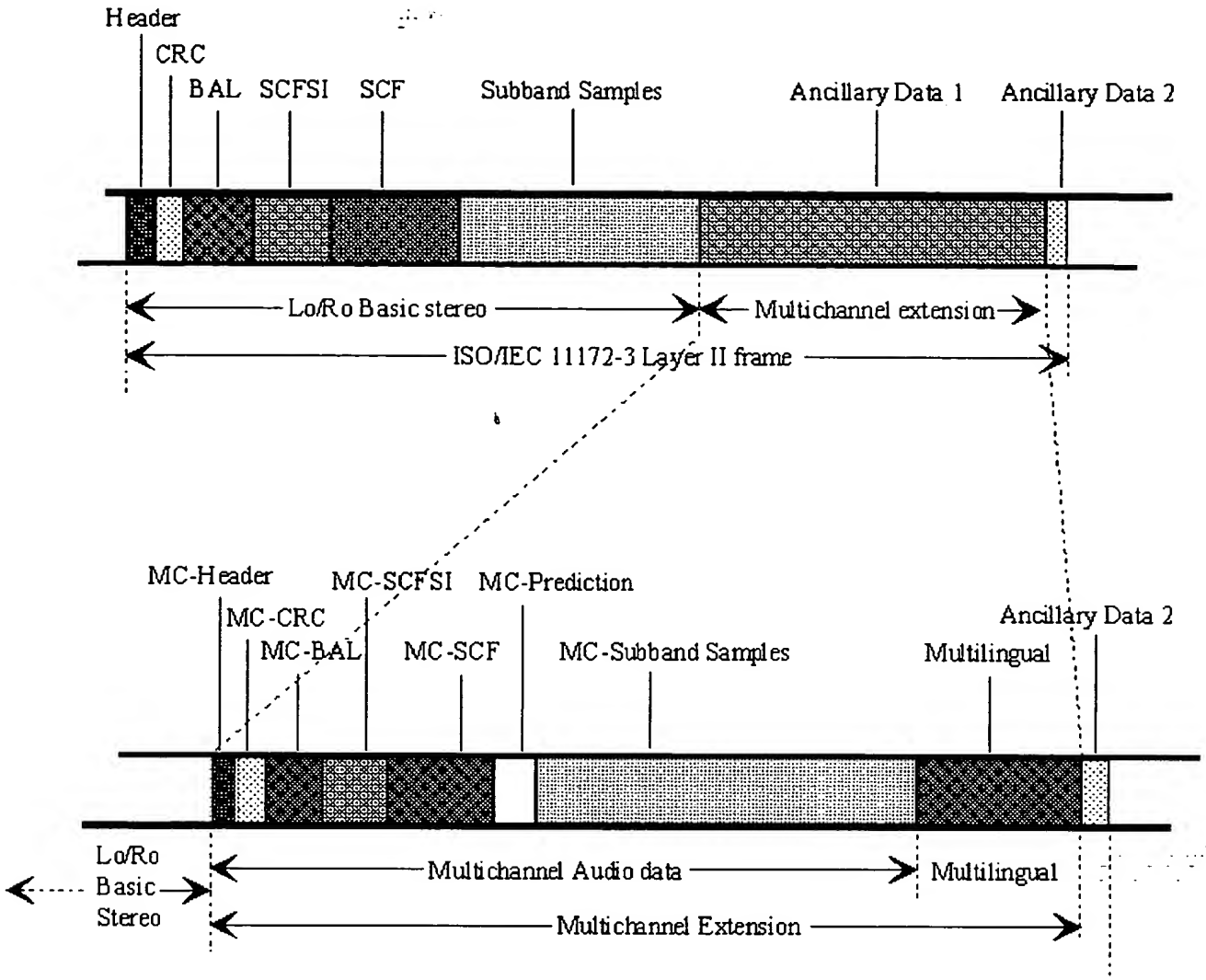


Figure 2 -- Structure of an MPEG-2 Audio block of data

Part 4 and 5 of MPEG-2 correspond to part 4 and 5 of MPEG-1. They have been finally approved in March 1996.

Part 6 of MPEG-2 - Digital Storage Media Command and Control (DSM-CC) is the specification of a set of protocols which provides the control functions and operations specific to managing MPEG-1 and MPEG-2 bitstreams. These protocols may be used to support applications in both stand-alone and heterogeneous network environments. In the DSM-CC model, a stream is sourced by a Server and delivered to a Client. Both the Server and the Client are considered to be Users of the DSM-CC network. DSM-CC defines a logical entity called the Session and Resource Manager (SRM) which provides a (logically) centralized management of the DSM-CC Sessions and Resources (see Figure 3).

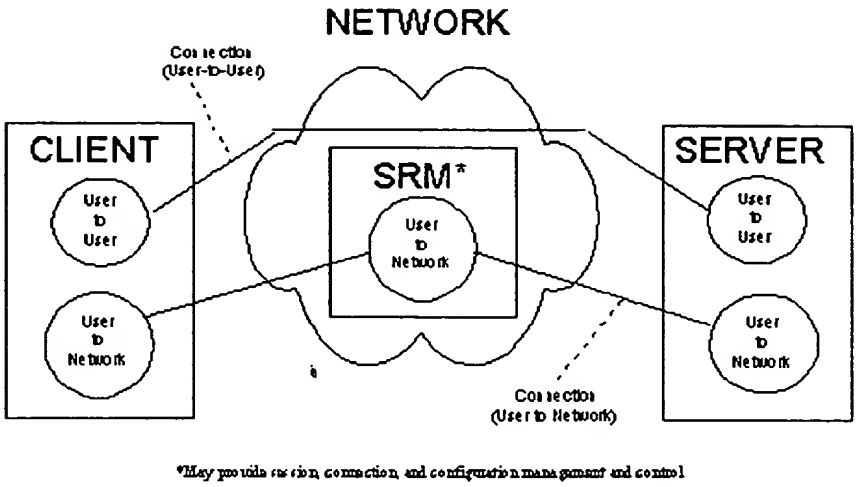


Figure 3 - DSM-CC Reference Model

Part 6 has been finally approved as an International Standard in July 1996.

Part 7 of MPEG-2 will be the specification of a multichannel audio coding algorithm not constrained to be backwards-compatible with MPEG-1 Audio. The standard has been approved in April 1997.

Part 8 of MPEG-2 was originally planned to be coding of video when input samples are 10 bits. Work on this part was discontinued when it became apparent that there was insufficient interest from industry for such a standard.

Part 9 of MPEG-2 is the specification of the Real-time Interface (RTI) to Transport Stream decoders which may be utilised for adaptation to all appropriate networks carrying Transport Streams (see Figure 4).

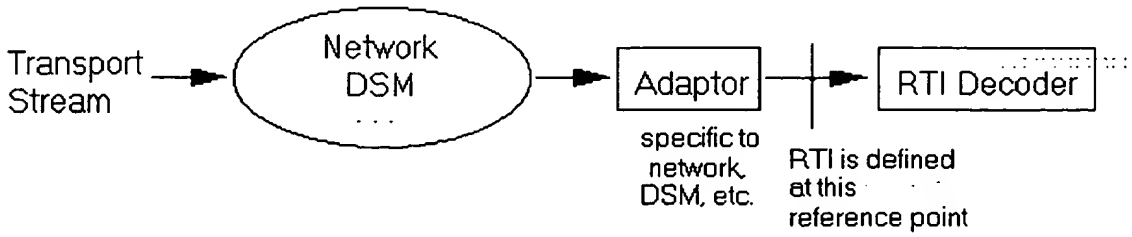


Figure 4 - Reference configuration for the Real-Time Interface

Part 9 has been finally approved as an International Standard in July 1996.

Part 10 is the conformance testing part of DSM-CC, under development.

held 5/11-1998 in Paris

OPEN PLATFORM INITIATIVE

for

MULTIMEDIA ACCESS

(OPIMA)

Call for Proposals for Technologies

Please note that proposers should:

• Notify their intention to submit a proposal on or before close of business of 24 August 1998 to leonardo.chiariglione@cselt.it

• Send their contribution by email on or before close of business of 31 August 1998 to leonardo.chiariglione@cselt.it. The contribution must be in Word 6, HTML or PDF format.

Table of Contents

Intellectual Property Rights Statement

When submitting a proposal, authors must acknowledge that in case part or all of their proposal is included in OPIMA specifications and the included part contains patented items which are necessary for the implementation of OPIMA specifications, the IPR owners will accept the IEC/ISO/ITU practice for patented items in international standards. This amounts to either giving free use of the patented items; or giving licence on fair and reasonable terms and on a non-discriminatory basis.

Model for Intellectual Property Rights Statement

The following model holds the key language of the IEC/ISO/ITU Intellectual property rights statement. It may be used as a basis to provide the required IPR statement:

<Company Name> hereby declares that it is prepared to license its IPR, both granted and pending, which is necessary to manufacture, sell and operate implementations of OPIMA specifications.

<Company Name> also declares that it is willing to grant a licence to an unlimited number of applications throughout the world under reasonable terms and under conditions that are demonstrably free of any unfair competition.

<Signature>

<Name and function of responsible company representative>

Executive summary

This Call for Proposals is an invitation to submit proposals for platform technologies needed to realise the OPIMA goal of a system where the consumer is able to obtain a terminal and begin to consume and pay for multimedia services, without having prior knowledge of which services would be consumed, in a simple way such as by operating a remote control device.

These proposed technologies are intended to be utilised in the development of a specification that may be used by content and service providers, and by manufacturers to enable services satisfying the definition above. The time scale of specification development is 1999.

Those intending to submit a proposal(s) should consult Section 6 of this Call for Proposals.

1. Introduction

Recent developments in digital techniques have stimulated the deployment of digital services that are attractive to users by virtue of their ability to offer improved functionalities compared to those of analogue technologies.

Protection of content is of paramount importance for the success of these new services. The current environment is one in which content protection systems are designed and deployed on a proprietary basis. While this satisfies the concerns of individual service providers, it often discourages consumers because devices employed to decrypt signals can perform their function only for one or a reduced number of service providers. Therefore users can access different service providers only by acquiring multiple terminal devices.

The Open Platform Initiative for Multimedia Access (OPIMA) is based on the belief that the multimedia market would see a faster development if a standardised technology existed that would allow a user to consume and pay for services, without having prior knowledge of which services would be consumed, in a simple way such as by operating a remote control device. Fig. 1 below graphically depicts the goal of the OPIMA initiative in which the consumer is able to use a single terminal to access a multiplicity of services from multiple providers.

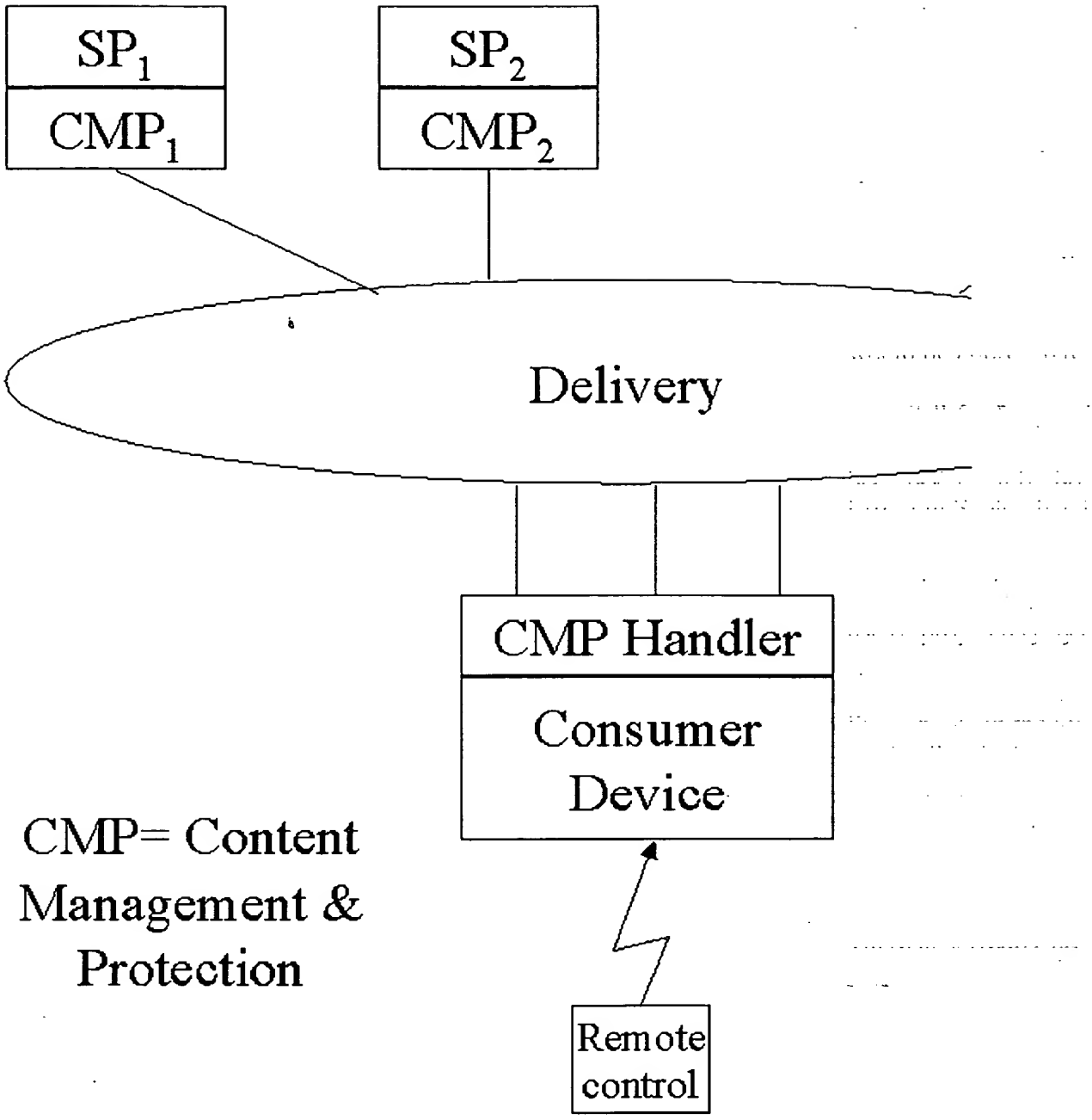


Fig. 1 - Graphical representation of the OPIMA goal

Even though the technology required to make possible the ideas described above exists, it is necessary to standardise some aspect of it in order to make the system work in an open manner. The international multi-industry OPIMA initiative has been established with the goal of achieving this standardisation. In this document "standardisation" is used to mean reaching industry agreement. It is envisaged that the OPIMA specification may be submitted to appropriate formal standards bodies for ratification.

This document has been developed by a group of industry representatives from different countries and

different components of the multimedia industry. It contains a list of possible applications and a list of requirements that it is believed need to be satisfied if the listed applications are to be supported. A very general reference model is given along with an analysis of how some of the existing solutions map onto the reference model.

The list of applications provided in this document is not necessarily exhaustive, and proposers may submit further applications if they feel that these would extend and improve the value of the specification. In this case proposers are invited to draw the attention to any additional requirements which arise from the additional applications.

The reference model has been kept at a very general level in order to minimise constraints placed upon any technology that a proposer may think appropriate. On the other hand proposers are invited to make the model more specific by providing further levels of detail of any technological components which would be appropriate for the attainment of the OPIMA goal.

This Call for Proposals is being widely disseminated to industry representatives and a wide range of responses is anticipated. At the September 1998 meeting the responses will be analysed and the technical work to develop the specifications will start. Current plans are that specifications will be frozen in September 1999.

While participants in the OPIMA initiative believe in the positive effect of the specifications on the development of the multimedia market, it is appreciated that different business models may require the use of proprietary systems. OPIMA has no intention of taking any action which would lead to the specifications becoming mandatory.

Participants in the OPIMA initiative are aware of the challenging nature of the current undertaking and invite all industry representatives sharing the OPIMA goal to join in this exciting technical development.

An electronic copy of this Call for Proposals can be found at

http://www.cselt.it/ufv/leonardo/opima

There is currently no plan to have a further call on the specific subject of this document. Therefore proposers should ensure that their contributions are submitted during this opportunity and comply with the deadlines specified.

2. OPIMA-enabled applications

2.1. List of Services to be supported

The services mentioned in this section serve as examples from which the requirements for the platform are derived. The specifications that OPIMA develops are targeted at supporting these services.

Note that while these examples imply certain business models, they do not make any assumption on the method of payment.

2.1.1. Required

Support for the following services and service models is required:

1. *Subscription TV/Audio*
2. *Pay-Per-Use*
3. *Near Video-on-Demand*
4. *Audio/Video-on-Demand*
5. *Services that add value* to those mentioned above – for example, paid-for Electronic Program Guides and other such services
6. *On-line multimedia services* – such as consuming services through the Internet
7. *Free TV/Radio* – the platform must allow free TV/Radio to be supported. *(Note that this is a requirement on the whole platform; not on any specific implementation. A service provider may choose an implementation that blocks the consumer device completely – and hence also block access to free TV/Radio – for example if a user does not pay for a subscription service)*

2.1.2. Optional

Additional services exist, which form an extension of the services mentioned under 'Required', and can be called 'Optional'. The following can be noted about these 'optionally supported services':

1. OPIMA believes the technology to allow the 'Required' services will naturally allow the 'Optional' services;
2. Technology proposed for supporting the Required services should not disallow the Optional services from being supported in the same system;
3. Proposals also supporting the Optional services, or allowing easy extension towards supporting them, will be evaluated more favourably than proposals only supporting the Required services.

These optionally supported services include:

- *Targeted advertising* – The user obtains permissions/credits in return for viewing advertising content
- *Rent-to-Own* – After paying *n* times, one can use the content for free (If $n = 1$, this becomes the 'Pay-One-Time-Fee' model)
- *Coupon Services* – The user gets a 'token' which may be used for using content, getting discounts, etc. The token can take many forms, for example a piece of software, a digital key, a smart card
- *Information services* – The content being obtained is not necessarily audiovisual. A few examples:
  - stock exchange information
  - traffic information
  - GPS information
- *Games* (single or multi user)
- *Software distribution* – It is believed that this is very similar to any other content distribution
- *Home shopping, home banking, gaming* – Services in which transactions play a role. Note that there is a clear connection between a television service (advertising) and home shopping
- *Auditing / Polling / Voting* – This means that a service provider can gain knowledge about the number of users accessing services and their degree of appreciation
- *Other services* – Please state which other services, not mentioned above, the proposal is also capable of supporting. Please address the question of how the proposal is open to newly developing services.

2.2. Benefit of the OPIMA approach to service integration

Currently a consumer who wants to access services from multiple providers is forced to have multiple terminals with different interfaces. This is an expensive and confusing situation, which slows down the adoption of digital services. The OPIMA initiative was launched to address this problem.

The OPIMA platform is primarily targeted to benefit consumers and service providers. Other players in the value network like rights holders, infrastructure and hardware providers may benefit from the platform as well, however always bearing in mind the benefits for the primary targets.

To encourage the provision of a greater selection of content to the consumer, the platform should guarantee the content providers' interests also through secure content management and protection and assurance of payment.

For a **consumer** it is of great benefit to have access to a platform that allows consumption of and easy payment for services, without having prior knowledge which services he would like to consume. For ease of use, these services should be provided on a single piece of equipment that is future-proof, following a consistent approach, controlled in a simple way such as by operating a remote control device. This consistent approach to services also relieves the consumer of complicated interaction concerning matters like authentication and payment.

For the **service provider** there is a standard interface to interact with all the terminals for all issues that deal with authentication, transaction processing and the like. Further, service providers could benefit from functionality like audits, polling, etc.

For the **hardware manufacturers** the OPIMA proposal offers the benefits of an open non-proprietary platform allowing fair competition. This of course also benefits the consumer.

It is recognised that the existence of such a platform would maximise the willingness of end users to consume content. This in turn would maximise content provisioning and globally enhance the role of **all legitimate actors** in the value network. The example of the GSM (Global System for Mobile) network and terminals has shown how standardisation can lead to economy of scale and enhanced service provision. It should be kept in mind, however, that the solution must be commercially viable and acceptable to the essential players in the network whose interests are impacted by any such solution.

It is important to note that OPIMA will propose specifications that interested parties are free to adopt. OPIMA does not intend to take any action which would lead to the specifications becoming mandatory.

3. Requirements

This section provides the requirements that guide the development of the OPIMA specifications. At the same time, it gives requirements for responses to this Call for Proposals (CfP). Sometimes a distinction is made between required support (usually denoted by the word 'shall') and optional support (usually expressed by using 'may').

3.1. Generic nature of the platform

The platform shall be as open as possible. In particular, the platform:

1. Preferably does not require proprietary hardware;
2. Preferably does not require a specific operating system.

3. Shall support multiple content management and protection systems (these individual content management and protection systems may, of course, use proprietary technologies, including hardware and software, as long as the interfaces conform to the OPIMA specifications).

3.2. Security and Privacy

The proposed platform needs to be secure and trustworthy. This means that:

1. The platform shall support identification and authentication of users and transactions (for example by digital contracts);
2. The platform shall prevent unauthorised access to information (i.e., access by parties that are not entitled to this information) and shall be robust against piracy. (Aspects of these requirements may be: preventing unauthorised copying of and access to content);
3. The platform shall support a means of assuring that users are only charged for services they have agreed to consume, and support giving the user an overview of the services consumed;
4. The platform shall support 'non-repudiation', i.e.:
    - o provide proof that the user has agreed to order / consume the service;
    - o provide proof of payment;
5. The platform shall support provision of accurate accounting information;
6. The platform may support – perhaps by providing some of the functionality listed above – binding negotiations. (This requirement refers to a model in which, if a party bids for goods or services using the platform, and the bid is accepted by the other party, this bid is equivalent to a purchase agreement.)

If different levels of security and robustness against piracy are allowed, systems with lower security levels shall never be able to compromise systems with higher security levels.

The platform shall support access control by

1. parental control;
2. jurisdictional and cultural policy (i.e., legal restrictions, possibly geographically determined).

The platform shall support service models in which the user's identity is not disclosed to the service provider and/or to other parties.

3.3. Connection type / form of interaction

This section lists requirements in the area of the type of connection and the form of interaction. Like before, there are requirements that *must* be supported, and extensions that, while they do not address the immediate focus of this Call for Proposals, do increase the value of the proposal.

The following types of connection shall be supported:

1. 1. Off-line consumption of content
2. 2. On-line consumption of content, for which are distinguished:

    a. Broadcast, with the following return channel characterisations:

    - o i) without return channel

- ii) with intermittent return channel
- iii) with persistent return channel

b. Interactive, with the following return channel characterisations:

- i) symmetric and asymmetric bandwidth
- ii) similar or different paths to and from the user

It is understood that these models and their sub-categories are not mutually exclusive.

Along a slightly different axis describing the connection, the platform shall be able to support:

1. *One-to-one operation*; such as sending content from a service provider to a user;
2. *One-to-many operation*; such as sending content to multiple users on a broadcast network;
3. *Many-to-one operation*; such as when a user receives content from several service providers simultaneously; the collection of information constitutes one consistent service.

Along the same axis, proposals *may* also support:

1. *Many-to-many*, like in multi-party games, in which value is at stake.

The platform shall at least support:

1. service provider to customer operation.

In addition, it may also support:

1. customer-to-customer operation, in which value is transferred from one (end) user to another;
2. service provider to service provider operation.

3.4. Types of transactions

The platform shall allow a wide range of transaction models. At least the following types of transactions shall be supported:

1. prepaid;
2. postpaid;
3. subscription;
4. pay-per-use;
5. rent-to-own;
6. booking;
7. credit and debit;
8. end user pays; third party pays; service provider pays (possibly to the end user);
9. incremental purchase of permissions with respect to the same content, for example: one first obtains the permission to *view*, and afterwards the permission to *modify* or *copy*.

Both on-line and off-line connection modes are foreseen with these types of transactions. Please indicate which types of transactions are supported for each of the connection modes.

Note: again it is recognised that these transaction models are not mutually exclusive.

3.5. Device types

A device is a system that is used to access and consume information. In principle, the platform shall support any device that can be used to consume multimedia services. At least the following devices need to be supported:

1. Digital TV
2. Set top boxes
3. Local storage devices (e.g., DVD-RAM)
4. Digital Radio
5. Personal Computers
6. Mobile devices used to access multimedia services
7. Screen telephones.

Support for other (future) multimedia devices may also be considered.

3.6. Mobility

The platform shall support mobility. In particular, it shall:

1. support service models that allow terminal mobility, meaning that the user can use the same device in different locations;
2. have provisions for supporting user mobility across terminals, meaning that the users can move to a different terminal and keep their permissions to use the service.

While user mobility could be provided through 'personalisation' and the usage of 'user profiles', this issue is considered to be outside the scope of this Call.

3.7. List of Parties / Roles in the Value Network

The focus of OPIMA is currently on the relationship between

- the end user, and
- the service provider.

OPIMA recognises that many other roles exist in the value network. The platform shall not exclude the interests of these parties from being served.

While this Call for Proposals is not focused on these other parties, proposers are asked to state how their proposal affects the position of these other parties. Also, OPIMA asks proposers to assess how silent OPIMA and the proposed solution can be about the existence of these parties.

These parties include:

1. Hardware manufacturers
2. Security providers

3. Service brokers
4. Rights holders
    - on content
    - on algorithms (e.g., coding algorithms)
5. Infrastructure providers
6. Transaction infrastructure providers
7. Legitimate third parties (Third parties such as trusted third parties, tax authorities, regulatory agencies, *not* including parties like pirates)
8. The end user in the role of service provider.

It is understood that several of these roles can be unified in one entity.

4. Reference Architecture

4.1. The OPIMA approach to specifications

The figure below is a representation of the system addressed by OPIMA specifications. It comprises four entities: the Service Provider System (SP), the Service Provider Support (SP') as seen from the end-terminal perspective, the trusted middleware (TMW); and the Smart Card (SC). In principle, OPIMA specifications can address any subsystem in a similar context.

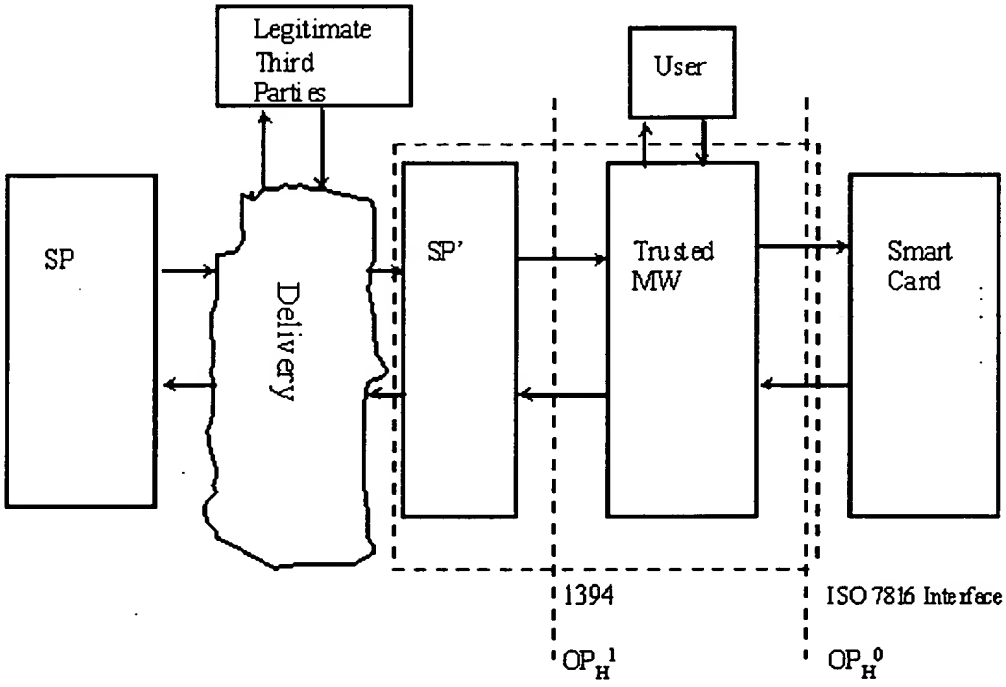


Fig. 2 - OPIMA Reference Model

Notes to the picture:

- *The 'H' in OP_HX refers to OPIMA Hardware*
- *Truted Middleware and Smart Card functions could also be carried together (e.g., on a PC card)*
- *Permissions are to be fully portable (e.g., on a Smart Card)*
- *Trusted Middleware is self-replaceable*
- *SP' is a generic service provider interface manufactured into every OPIMA device.*

Relocation of tools. Because OPIMA specifications have to satisfy business and service models of multiple industries, OPIMA tools need not only to be usable in a variety of different systems but also in different parts of the same systems. OPIMA defines its tools in such a way that they can be relocated, whenever this relocation is technically possible and practically meaningful.

OPIMA specifies the minimum. If the OPIMA reference model is mapped onto a particular application, the boundaries shown in the diagram may not be identifiable. As OPIMA addresses a multi-industry environment, it can only produce specifications of tools with the minimum of detail needed for interoperability.

The OPIMA architecture is intended to have longevity. The technologies used by OPIMA systems are targets for attack by illegal operators and interests. Therefore, the technology and the nature of the tools that will be used by OPIMA conformant systems require flexibility and the ability to replace components as they are compromised or when better technology becomes available.

4.2. Assumptions

The following assumptions reflect a basic rationale behind the elements of the OPIMA reference architecture:

Assumptions	Benefits
1. A secure and trusted environment in which all implementations are based	Service provider confidence
2. Intellectual property is protected	Content owner confidence
3. No predefined location and implementation of API's and hardware interfaces	Multiple instantiations of the architecture with a variety of exposed interfaces
4. Existence of user identification module	Unique identification of users whilst protecting privacy
5. Existence of a secure dynamic (distributed) registry for hardware and software interfaces	Uniform manufacturing; Local configuration and personalisation

4.3. Elements of the reference model

Smart Card (SC)

The smart card is viewed as the user identification and service enabling module. The smart card may be provided to a consumer by a Service Provider or an independent vendor. It should not be limited to enabling access to a single service provider or to a single application. The smart card should be a secure

environment in which the consumer is confident of its integrity. The currently known interface for smart card technology is given in ISO 7816 and its subchapters.

Service Provider System (SP) and Service Provider Support (SP')

The service provider is an entity which presents a unified image to a consumer who wishes to consume the services or products offered by the service provider. A service provider may have unique and proprietary applications requirements and interfaces. These are made transparent to the consumer by a secure download technology enabled by an OPIMA compliant terminal. This is accomplished by the presence of a generic (and secure) service provider support function (SP') in combination with a trusted middleware component (TMW) that is resident in each OPIMA compliant terminal at the time of manufacture.

Legitimate Third Party

A legitimate third party (LTP) is an entity whose presence in the system is authorised. This excludes unauthorised third parties such as pirates. The presence of an LTP is optional.

Trusted Middleware (TMW)

Trusted Middleware (TMW) is the core element in the system's ability to provide secure and trusted services. Only a certified middleware component has the ability to incorporate and certify additional or replacement functionalities including replacing itself in a trusted manner.

The trusted middleware component is capable of communicating with the smart card and the service provider support functions. The trusted middleware component manufactured within each OPIMA terminal contains the necessary functions to facilitate the addition of the Service Provider elements of the TMW. This can be achieved via secure download or other trusted methodology. The basic TMW, without any additional elements, will allow the operation of the basic functions for which the terminal is intended. For example, a digital television without these additional elements can receive and display free TV services.

Functions that are specific to individual Service Providers may be added to the basic TMW. This allows one or more service providers to offer available services on an OPIMA terminal. Security and application protection and management are required when additional service enabling is provided.

The SP' and TMW functionality may be combined in a single entity. If they are not, an interface such as IEEE 1394 may be used.

4.4. Known hardware Specifications

For the interfaces depicted in the diagram above, the following interfaces are known:

OP_H1	IEEE 1394 (CPT WG-1)
OP_H0	ISO 7816

5. Example implementations

In this section we show how two different implementations can be mapped onto the reference model above.

5.1. Global System for Mobile (GSM)

This section describes the application of a GSM-like Challenge/Response Scenario to the OPIMA Reference Model.

5.1.1. Description of GSM security mechanisms

The security services provided by GSM are:

- *Anonymity* – Making it difficult to identify the user of the system to parties that are not entitled to this information.
- *Authentication* – To identify the user to the service provider for billing purposes.
- *Signalling Protection* – To protect sensitive information on the transmission channel.
- *User Data Protection* – To protect the passing of user data across the network.

The use of a SIM (Subscriber Identity Module) card is central to the security model of GSM. The GSM system goes through a number of steps to ensure secure use of services:

- Equipment Authentication
- SIM Verification
- SIM Authentication
- Secure Payload Exchange.

1. Equipment Authentication

As each GSM Mobile Terminal has a unique identity (IMEI, International Mobile Equipment Identifier); the first step after connection to the service network is to check the terminal is not blacklisted.

2. SIM Verification

The purpose of this step is to increase probability that the SIM is in the hands of the correct user. This is done by prompting the user for a secret code (PIN), which is checked locally on the SIM.

3. SIM Authentication

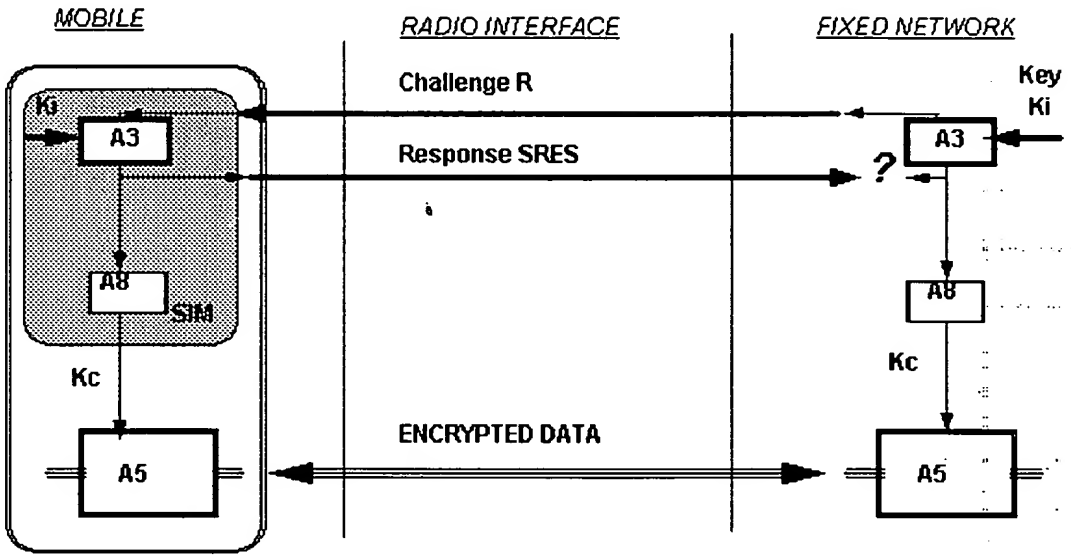
Authentication involves two functional entities: The SIM card in the Mobile Terminal and the Authentication database of the service provider. Each subscriber is given a secret key, a copy of which is stored in the SIM card and in the Authentication database. During the authentication process, the service provider generates a random number to the terminal. Both the mobile terminal and the service provider then use the random number and the secret key to compute, through a commonly agreed ciphering algorithm a so called Signed Response (SRES), which the mobile terminal sends back to the service provider. If the two computed numbers are the same, the subscriber is authenticated.

For authentication of Internet access over dial-up links where the PPP is used, a similar mechanism is used as defined in RFC 1994.

4. Secure Payload Exchange

The same SRES is then used to compute, using a second algorithm, a ciphering key that will be used for payload encryption / decryption, using a third algorithm.

The process is illustrated by the following diagram:



5.1.2. Mapping GSM system elements to OPIMA system elements

GSM	OPIMA
SIM	Smart Card / User Identification Module
Mobile Terminal (MT)	Consumer Device
MT Implementation	Trusted Middleware (TMW)
Currently no downloading - SIM Toolkit (future)	SP' (download)

GSM's Subscriber Identity Module corresponds to OPIMA's Smart Card, or, more generally, a OPIMA User Identification Module.

The OPIMA consumer device, including the software in it, corresponds to the GSM mobile terminal. The essential difference is that GSM terminals currently do not support software download from the service provider (although this is an ongoing development), which is on the other hand a crucial capability of the OPIMA consumer device.

For that reason, the TMW (Trusted Middleware) is mapped to the Mobile Terminal implementation, whereas the SP' element currently has no direct correspondence on the GSM model.

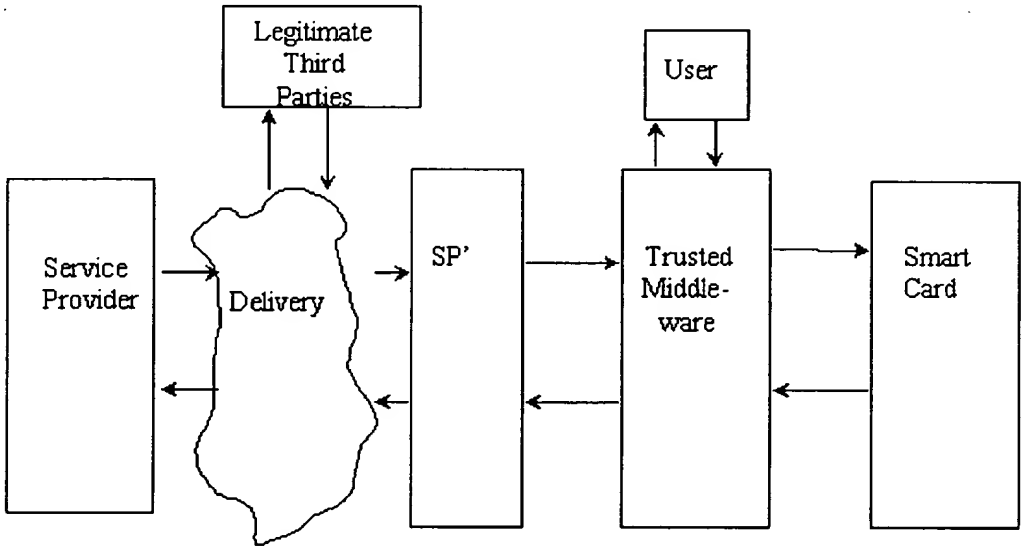
5.1.3. GSM-like authentication applied to OPIMA reference model

The user authentication procedure allowed by the OPIMA reference model is as follows:

1. If the OPIMA consumer device is newly purchased without preloaded Service Provider specific elements, we assume the consumer device only has the basic capability to connect to some service

provider and to support basic secure download.
2. It is assumed that the Smart Card / User Identification Module is inserted in the consumer device.
3. The user is optionally asked for card verification, by prompting for entry of a secret code (PIN).
4. The consumer device connects to a service provider. It is assumed that the Smart Card was issued by the service provider and thereby determines the primary service provider the consumer device connects to.
5. The consumer device transmits the identity of the user (and optionally of the equipment) to the service provider.
6. The Service Provider transmits a random number to the consumer device in order to initiate user authentication.
7. The Trusted Middleware and the service provider simultaneously compute a Signed Response (SRES) from the random number and the user-specific secret key, using a commonly agreed algorithm.
8. The terminal sends the SRES to the service provider, who compares the two numbers.
9. If the two numbers are equal, the authentication was successful.
10. The same initial random number and subscriber key can be used to compute another key using another algorithm, to encrypt / decrypt payload if desired.

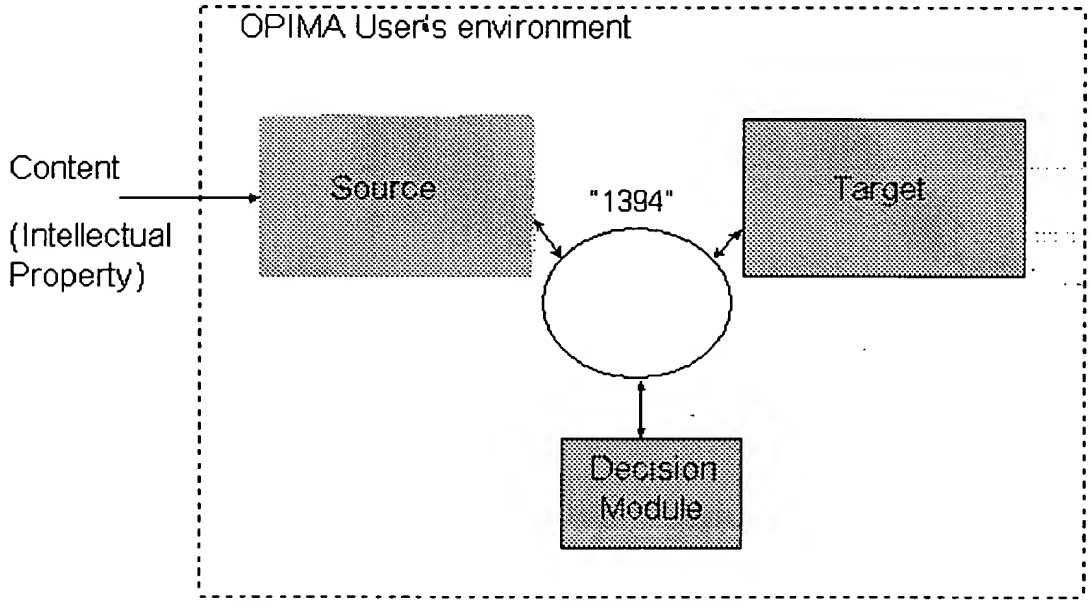
In the following interaction diagram, system elements which only pass information through such as the delivery network and the SP' component, are omitted.



5.2. Intellectual Property Management and Protection Framework / "You Play-You Pay"

Another possible scenario for use of the OPIMA Reference Model is in providing protection and management of intellectual property, both in content and, potentially algorithms and other components of the environment.

Such uses highlight the potential diversity of the applications, as some intellectual property owners may wish to use only the most rudimentary protection schemes, whilst others may wish to employ much more complex approaches involving both management and protection.



Intellectual Property Manangement and Protection Framework

OPIMA User Environment: This could represent, for example, the user's home appliances, interconnected by a 1394-like bus, as being considered by the Multimedia Home Platform activity of the DVB project.

"1394" bus: Allows establishing of secure point-to-point channels (by performing authenticated key exchange (AKE) and encryption/decryption). [IEEE 1394]

Source: Is a device which receives content from outside the environment (e.g. by broadcast, internet, phone or physical media such as DVD disc). It could be, for example, a receiver or an Integrated Receiver/Decrypter (IRD).

Target: Is a device which is the final destination of the content where the content is consumed. It could be a digital television display or a recording device, such as DVD-RAM.

Decision Module: Is a device responsible for deciding whether the transmission of the content from the source to the target is permitted. In particular the decision module might verify the credentials of the other modules and the proper matching of authorizations to these credentials. These authorizations may come with the content over any of the available channels and must somehow be securely associated with the content. One possible implementation of the decision module is a tamper-resistant smart card which

allows periodic upgrades.

Any of the components above could be a software module in a PC.

How does intellectual property management and protection (IPMP) operate in this scenario? In the extreme case (referred to by some as "You Play, You Pay"), used mainly for illustration, the content may come entirely unencrypted, but the decision module may refuse transmission from source to target unless it receives also proper authorisations for this transmission (e.g. a receipt of purchase, which could have been received offline from a retail store or over the phone or stored on a user's personal smart credit card).

5.2.1. Possible extensions

The above scenario can, in principle, be generalized to an arbitrarily complex, dynamic, distributed architecture.

In this architecture the necessary components could be specified by authorizations and/or other modules received from any source, thereby supporting dynamically re-configurable webs of trust. In particular some of the components could be implemented and delivered as software which is then run on trusted virtual machines. In this way the overall system security and flexibility can be increased, forcing the prospective pirate to compromise multiple and possibly dynamic points of the system. The architecture could even support secure intelligent agents e.g. performing negotiations etc. This approach also allows decisions about the optimal configurations of the system to be decided dynamically by market forces.

5.2.2. Mapping the IPMP Framework to the OPIMA Reference Model

The Source receives Content (Intellectual Property) from the Delivery cloud in the OPIMA Reference Model (RM). The relevant parts of Source and Target (in this case the IEEE 1394 interface) are part of the Trusted MW which must be integrated into components outside of the OPIMA RM (e.g. a digital TV display). Both Source and Target could be either the SP' or part of the Trusted MW or a combination of these two. The Decision Module maps to the Smart Card component. In this example the Trusted MW component of the RM is distributed in a number of interconnected Consumer Electronics components.

6. Submission, Evaluation and Subsequent Specification Development

Parties interested in proposing technology to OPIMA should:

1. Notify their intention to submit a proposal on or before close of business of 24 August 1998 to leonardo.chiariglione@cselt.it.
2. Send their contribution by email on or before close of business of 31 August 1998 to leonardo.chiariglione@cselt.it. The contribution must be in Word 6, HTML or PDF format.

Submissions will be posted on a password protected Web page for access by OPIMA participants. Those who do not wish to have their submission posted should state so in their submission but still need to send an electronic copy to the address above. In this case proposers shall bring 100 paper copies to the meeting place.